Amendments to the Claims

This listing of claims will replace all prior versions, and listings of claims, in the application.

Listing of Claims:

1. (Currently amended) A method for ~~annotating~~ labeling a query email message, the method comprising ~~the~~ steps of:

assigning attributes to at least one of a plurality of patterns based on prior email messages;

creating a pattern database comprising the plurality of patterns derived from and associated with an annotated database comprising SPAM email messages, and attributes representing features of the annotated database; and wherein each pattern occurs two or more times in the annotated database;

receiving the query email message;

accessing the pattern database to retrieve patterns with the assigned attributes that match the query email message ~~patterns associated with a database comprising annotated email messages;~~

~~assigning attributes to the patterns based on the annotated email messages; and~~

using the patterns with assigned attributes to analyze the query email message to determine whether the query email message is a SPAM or a non-SPAM email; and

labeling the query email message as SPAM or non-SPAM as determined from the analysis.

2. (Original). The method of claim 1, wherein the step of accessing patterns comprises using a pattern discovery algorithm.

3. (Currently amended) The method of claim 2 ~~1~~, wherein the pattern discovery algorithm is the Teiresias pattern algorithm.

4. (Original) The method of claim 1, wherein the steps of accessing patterns and assigning attributes are carried out independently of and prior to the step of using the patterns with assigned attributes to analyze the query email message.

5. (Canceled)

6. (Currently amended) The method of claim 1, further comprising ~~the~~ a step of storing the patterns with assigned attributes in [[a]] the pattern database.

7. (Currently amended) The method of claim 1, wherein the using step further comprises ~~the~~ a step of defining an attribute vector from the patterns with assigned attributes, the attribute vector characterizing portions of the query email message.

8. (Currently amended) The method of claim 1, wherein the using step further comprises ~~the~~ a step of defining an attribute vector from the patterns with assigned attributes, the attribute vector characterizing the whole of the query email message.

9. (Original) The method of claim 1, wherein one or more of said annotated email messages comprises an unwelcome email message ("SPAM").

10. (Currently amended) The method of claim 9, further comprising the step of storing the patterns with assigned attributes in [[a]] the pattern database ~~serving as a "SPAM dictionary"~~.

11. (Currently amended) The method of claim 1, wherein one or more of ~~said annotated~~ the labeled query email messages comprises a welcome email message ("non-SPAM").

12. (Currently amended) The method of claim 11, further comprising ~~the~~ a step of storing the patterns with assigned attributes in [[a]] the pattern database ~~serving as a "SPAM dictionary"~~.

13. (Currently amended) The method of claim 1, wherein ~~said~~ the annotated database comprises (i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and (ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM").

14. (Original) The method of claim 7, wherein the attribute vector comprises a number of counters.

15. (Original) The method of claim 14, wherein the query email message comprises characters of a human language and the number of counters is proportional to the number of said characters in the query email message.

16. (Original) The method of claim 14, wherein the assigned attributes are used to contribute values to counters of the attribute vector corresponding to portions of the query email message matched by the patterns.

17. (Original) The method of claim 7, comprising a plurality of attribute vectors.

18. (Original) The method of claim 17, wherein the values contributed to the counters of each of the attribute vectors of the plurality of attribute vectors are normalized.

19. (Original) The method of claim 17, wherein each attribute vector of the plurality of attribute vectors represents a different attribute.

20. (Original) The method of claim 17, wherein the plurality of attribute vectors are ranked.

21. (Original) The method of claim 20, wherein only highly ranking attribute vectors are kept.

22. (Currently amended) The method of claim 1, further comprising ~~the~~ a step of determining a score for the patterns with assigned attributes used to contribute to the attribute vector.

23. (Currently amended) The method of claim 22, wherein the determined score represents a degree of similarity between the query email message and at least one annotated email message of the database.

24. (Original) The method of claim 23, wherein the score is normalized.

25. (Original) The method of claim 22, wherein the score represents a degree of similarity between the query email message and at least one annotated email message of the database, and wherein said at least one of said annotated email messages comprises an unwelcome email message ("SPAM").

26. (Original) The method of claim 22, wherein the score represents a degree of similarity between the query email message and at least one annotated email message of the database, and wherein said at least one of said annotated email messages comprises a welcome email message ("non-SPAM").

27. (Currently amended) The method of claim 1, further comprising ~~the~~ a step of

determining a score for the patterns with assigned attributes used to contribute to the attribute vector, said annotated database comprising (i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and (ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM"), said score representing a degree of similarity[[,]] between the query email message and at least one of said annotated unwelcome email messages ("SPAM"), and a degree of dissimilarity between the query email message and at least one of

said annotated welcome email messages ("non-SPAM").

28. (Currently amended) The method of claim 27, further comprising ~~the~~ a step of

defining, for each of said assigned attributes, a value criterion based on the value of the counters of the attribute vector to determine whether the corresponding attribute is present in the query email message.

29. (Currently amended) The method of claim 27, further including ~~the~~ a step of

defining a SPAM attribute criterion dependent on which of said assigned attributes are present in the query email message, to determine whether the query email message is a SPAM email message.

30. (Currently amended) The method of claim 27, further including ~~the~~ a step of

defining a non-SPAM attribute criterion dependent on which of said assigned attributes are present in the query email message, to determine whether the query email message is a non-SPAM email message.

31. (Currently amended) An apparatus for ~~annotating~~ labeling a query email message, the apparatus comprising:

a memory comprising a pattern database, the pattern database comprising a plurality of patterns derived from and associated with an annotated database of known SPAM email messages, and attributes representing features of the annotated database; and wherein each pattern occurs two or more times in the annotated database; and

at least one processor, coupled to the memory, operative to:

assign attributes to at least one of a plurality of patterns based on the query email message;

access the pattern database to retrieve patterns with the assigned attributes that match the query email message ~~patterns associated with a database comprising annotated email~~

~~messages~~;

~~assign attributes to the patterns based on the annotated email messages~~; ~~and~~

use the patterns with assigned attributes to analyze the query email message to determine whether the query email is a SPAM or a non-SPAM email; and

label the query email message as SPAM or non-SPAM as determined from the analysis.

32. (Previously presented) The apparatus of claim 31, wherein the at least one processor is further operative to select the accessed patterns that match patterns in the query email message.

33. (Original) The apparatus of claim 31, wherein in accordance with the using operation the at least one processor is further operative to define an attribute vector from the patterns with assigned attributes, the attribute vector characterizing portions of the query email message.

34. (Original) The apparatus of claim 31, wherein at least one of said annotated email messages comprises an unwelcome email message ("SPAM").

35. (Original) The apparatus of claim 31, wherein at least one of said annotated email messages comprises a welcome email message ("non-SPAM").

36. (Currently amended) The apparatus of claim 31, wherein said annotated database comprises

(i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and

(ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM").

37. (Original) The apparatus of claim 33, wherein the attribute vector comprises a number of-counters.

38. (Original) The apparatus of claim 37, wherein the query email message comprises characters

of a human language and the number of counters is proportional to the number of said characters in the query email message.

39. (Original) The apparatus of claim 37, wherein the assigned attributes are used to contribute values to counters of the attribute vector corresponding to portions of the query email message matched by the patterns.

40. (Original) The apparatus of claim 33, comprising a plurality of attribute vectors.

41. (Original) The apparatus of claim 39, wherein each attribute vector of the plurality of attribute vectors represents a different attribute.

42. (Original) The apparatus of claim 39, wherein the plurality of attribute vectors are ranked.

43. (Original) The apparatus of claim 31, wherein the at least one processor is further operative to determine a score for the patterns with assigned attributes used to contribute to the attribute vector.

44. (Currently amended) The apparatus of claim 43, wherein the score represents a degree of similarity between the query email message and the annotated email messages of the annotated database.

45. (Currently amended) The apparatus of claim 43, wherein the score represents a degree of similarity between the query email message and at least one of the annotated email messages of the annotated database, and wherein said at least one of said annotated email messages comprises an unwelcome email message ("SPAM").

46. (Currently amended) The apparatus of claim 43, wherein the score represents a degree of

similarity between the query email message and at least one of the annotated email messages of the annotated database, and wherein said at least one of said annotated email messages comprises a welcome email message ("non-SPAM").

47. (Currently amended) The apparatus of claim 31, wherein the at least one processor is further operative to determine a score for the patterns with assigned attributes used to contribute to the attribute vector, said annotated database comprising (i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and (ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM"), said score representing a degree of similarity, between the query email message and said annotated unwelcome email messages ("SPAM"), and a degree of dissimilarity between the query email message and said annotated welcome email messages ("non-SPAM").

48. (Currently amended) An article of manufacture for ~~annotating~~ labeling a query email message, comprising a machine readable medium containing one or more programs which when executed implement ~~the~~ steps of:

assigning attributes to at least one of a plurality of patterns based on the query email message;

creating a pattern database comprising the plurality of patterns, derived from and associated with an annotated database of known SPAM messages, and attributes representing features of the annotated database and wherein each pattern occurs two or more times in the annotated database;

accessing the pattern database to retrieve patterns with the assigned attributes that match the query email message ~~patterns associated with a database comprising annotated email messages~~;

~~assigning attributes to the patterns based on the annotated email messages; and~~

using the patterns with assigned attributes to analyze the query email message to determine whether the query email message is a SPAM or a non-SPAM email; and

labeling the query email message as SPAM or non-SPAM as determined from the analysis.

49. (Currently amended) The article of manufacture of claim 48, further comprising ~~the~~ a step of selecting the accessed patterns that match patterns in the query email message.

50. (Original) The article of manufacture of claim 48, wherein the using step further comprises defining an attribute vector from the patterns with assigned attributes, the attribute vector characterizing portions of the query email message.

51. (Original) The article of manufacture of claim 48, wherein at least one of said annotated email messages comprises an unwelcome email message ("SPAM").

52. (Original) The article of manufacture of claim 48, wherein at least one of said annotated email messages comprises a welcome email message ("non-SPAM").

53. (Currently amended) The article of manufacture of claim 48, wherein said annotated database comprises (i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and (ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM").

54. (Original) The article of manufacture of claim 50, wherein the attribute vector comprises a number of-counters.

55. (Original) The article of manufacture of claim 54, wherein the query email message comprises characters in a human language and the number of counters is proportional to the number of said characters in the query email message.

56. (Original) The article of manufacture of claim 54, wherein the assigned attributes are used to contribute values to counters of the attribute vector corresponding to portions of the query email message matched by the patterns.

57. (Original) The article of manufacture of claim 50, comprising a plurality of attribute vectors.

58. (Original) The article of manufacture of claim 57, wherein each attribute vector of the plurality of attribute vectors represents a different attribute.

59. (Original) The article of manufacture of claim 57, wherein the plurality of attribute vectors are ranked.

60. (Currently amended) The method of claim 48, further comprising ~~the~~ a step of determining a score for the patterns with assigned attributes used to contribute to the attribute vector.

61. (Currently amended) The article of manufacture of claim 60, wherein the score represents a degree of similarity between the query email message and the annotated email messages of the annotated database.

62. (Currently amended) The article of manufacture of claim 60, wherein the score represents a degree of similarity between the query email message and at least one of the annotated email messages of the annotated database, and wherein said at least one of said annotated email messages comprises an unwelcome email message ("SPAM").

63. (Currently amended) The method of claim 60, wherein the score represents a degree of similarity between the query email message and at least one of the annotated email messages of the annotated database, and wherein said at least one of said annotated email messages comprises a welcome email message ("non-SPAM").

64. (Currently amended) The article of manufacture of claim 50, further comprising ~~the~~ a step of determining a score for the patterns with assigned attributes used to contribute to the attribute vector, said annotated database comprising (i) a first subdatabase comprising annotated unwelcome email messages ("SPAM"), and (ii) a second subdatabase comprising annotated welcome email messages ("non-SPAM"), said score representing a degree of similarity[[,]] between the query email message and at least one of said annotated unwelcome email messages ("SPAM"), and a degree of dissimilarity between the query email message and at least one of said annotated welcome email messages ("non-SPAM").